Neues Rating-System für Sicherheitsfehler vorgestellt

Mehrere Sicherheitsdienstleister unter dem Dach des FIRST (Forum of Incident Response and Security Teams) haben US-amerikanischen Medienberichten zufolge ein neues Rating-System zur Risikoeinschätzung von Sicherheitslücken namens *Common Vulnerability Scoring System* (CVSS) vorgestellt. Das System wurde unter der Federführung des amerikanischen National Infrastructure Advisory Council in den vergangenen anderthalb Jahren entwickelt und seit Ende Februar von 30 nicht näher genannten Unternehmen getestet.

Nun sucht das FIRST nach weiteren Unternehmen, die das System einsetzen wollen. CVSS geht über die derzeit üblichen Rating-Mechanismen hinaus. Diese kennen bislang beispielsweise wie bei Microsoft nur Stufen wie "wichtig" und "kritisch". Das neue System nutzt Zahlen zwischen 1 und 10 und soll es Unternehmen durch weitergehende Informationen ermöglichen, das Risiko für die eigene Infrastruktur besser einzuschätzen. Damit ließe sich das Patch-Management der im Einsatz befindlichen IT-Infrastruktur angemessen priorisieren.

In das CVSS-Rating fließen sowohl grundlegende Bewertungen (basic metrics) wie lokale oder entfernte Ausnutzbarkeit der Lücke ein als auch zeitliche Komponenten (temporal metrics) wie die Verfügbarkeit eines Exploits oder die Vertrauenswürdigkeit der Schwachstellen meldenden Instanz. Zu guter Letzt wird noch die System-Umgebung der Lücke (environment metrics) gewichtet, beispielsweise über physische Auswirkungen oder die Anzahl möglicher verwundbarer Systeme. Im FAQ des CVSS werden die einzelnen Kriterien näher beleuchtet.

Als eines der ersten großen Unternehmen stellt Cisco auf der MySDN-Sicherheitsseite CVSS-Scores zur Verfügung – allerdings nicht in seinen eigenen Advisories. Als weitere große Unternehmen sollen den Berichten zufolge Symantec, Internet Security Systems und Qualys auf den CVSS-Zug aufspringen. Interessant ist Microsofts Standpunkt: Die Redmonder wollen das neue System vorerst nicht aufgreifen, sondern erst auf größere Nachfrage von Kunden hin.

Damit würde das System von vornherein in der Verbreitung gebremst, orakelt der Gartner-Vizepräsident John Pescator gegenüber US-amerikanischen Medien. Er verlautbart auch, dass die Hilfestellung bei der Priorisierung der Patches überbewertet wird. Kein Rating-System könne dies leisten, dennoch wäre es gut für die IT, ein solches zu haben.

Bisherigen proprietären Rating-Systemen zur Risikoeinschätzung von Sicherheitslücken ist gemeinsam, dass sich keines davon als überlegen erwiesen hat oder sich durchgesetzt hätte – jeder Sicherheitsdienstleister kocht noch immer sein eigenes Süppchen. Dies könnte sich nun ändern, da tatsächlich einige Branchengrößen das neue CVSS einsetzen wollen. Dennoch bleibt es Aufgabe jedes einzelnen IT-Verantwortlichen, seine eigene Risikoeinschätzung zu machen, da sich die eigene Infrastruktur zumeist von dem Durchschnitt, der dem CVSS in den Environment Metrics zugrundeliegt, unterscheidet.